ID Theft & Phishing

How Phishing Works:

Phishing (pronounced fishing) is a form of identity theft in which identity thieves "fish" for your personal information by sending e-mail or spam messages which appear to come from a reputable company you deal with on a regular basis. These e-mails typically use scare tactics to notify you of a "serious" problem which requires your immediate attention. The e-mails generally include one or more links to a company's website. In a phishing scam, you would be redirected to a phony website made to look exactly like the real thing. They may then ask you to update your personal or account information. Do not provide this information, unless you have initiated the communication.

Internet and Computer Safety Tips:

- When entering a secure site, you should see https:// in the navigation bar and a security padlock (🔒) on the screen. Currently, the "s" in combination with the padlock, indicates that the site is secure.
- Be careful about clicking on Web links sent via e-mail. Never click on a link sent in an unsolicited e-mail. When sending personal or financial information via e-mail, be sure your message is encrypted.
- Create unique passwords and change them frequently. Avoid using passwords such as your birth date, name, address, or Social Security number. Use a combination of upper and lowercase letters, numbers and special characters.
- If your computer prompts you to "save" or "store" a password, decline. Allowing your computer to remember login information gives anyone with physical access to your computer the ability to log in to your accounts.
- Keep your computer anti-virus software up to date in order to effectively guard against new viruses. Maintain current versions of your computer's operating system, Internet browsers, and application software.

Verifying and Protecting Your Identity:

To protect yourself and your family from identity theft and related crimes:

- Review all account statements. Notify us immediately should you see any discrepancies in your accounts with us.
- Shred financial documents and paperwork containing personal information before disposing of them.
- Keep track of credit, debit, and ATM card numbers and store this information in a secure location. Report any lost or stolen checks, debit or credit cards to your financial institution or credit card company.
- Do not carry your Social Security card, or number, with you.

If You Are Victimized:

If you determine your identity has been stolen, immediately contact the local police department to file a police report. Also, contact each of the credit reporting agencies to place a "Fraud Alert" on your credit report, as well as any parties with whom you have a financial relationship. The three major credit reporting agencies are:

- Equifax
  1.800.525.6285
  www.equifax.com

- Experian
  1.888.397.3742
  www.experian.com

- TransUnion
  1.800.680.7289
  www.tuc.com

FDIC

406 Bay Street, Petoskey Michigan 49770
877.487.1765 www.tbonm.com

130 South Union Street, Traverse City Michigan 49684
866.237.7999 www.tbonm.com

THE BANK OF
northern michigan